1994-12

ECCM networking research

Chang, Eugene King

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/30805

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

ECCM NETWORKING RESEARCH

by

Eugene King Chang

December, 1994

Thesis Advisor: Alex W. Lam

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1 AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 1994	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE ECCM NETWORKING RESEARCH	5. FUNDING NUMBERS
6 AUTHOR(S) Eugene King Chang	
7 PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11 SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

Spread-spectrum modulation techniques, which are traditionally applied to military systems to enhance their Electronic Counter Counter Measures (ECCM) capabilities, are beginning to appear in the commercial sector. Specifically, spread-spectrum technology is being employed in digital cellular radio systems. These systems are identical to the military systems except that they employ much simpler spreading code design and have less security incorporated. However, due to the economies of scale, they can be produced at a much lower cost than their military counterparts.

The jamming vulnerability of such commercial products in tactical situations is analyzed in this thesis. The mobile cellular network developed by Qualcomm Inc. is used to illustrate the methodology in analyzing the effects of jamming on the mobile cellular network. With a single mobile station and jammer, the probability of jamming and the optimal jammer trajectory are derived. Next, the effective probabilities of detection and false alarm under the jamming conditions are derived and the mean acquisition times are compared to that without jamming. Our results show that intelligent jamming can cause devastating effects even with very small power. Commercial products are therefore much more vulnerable due to the simplicity in design.

14. SUBJECT TERMS Spread-spectrum, acquisition, mean time to acquire, code division multiple access (CDMA), intelligent jamming, cellular mobile communications, digital communications.	15. NUMBER OF PAGES 75
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited.

ECCM NETWORKING RESEARCH

by

Eugene King Chang
Major, Republic of Singapore Air Force
B.Eng.(Hons), National University of Singapore, 1986

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 1994

Author: [redacted]
Eugene King Chang

Approved by: [redacted]
Alex W. Lam, Thesis Advisor

[redacted]
Donald v. Z. Wadsworth, Second Reader

[redacted]
Michael A. Morgan, Chairman,
Department of Electrical and Computer Engineering

ABSTRACT

Spread-spectrum modulation techniques, which are traditionally applied to military systems to enhance their Electronic Counter Counter Measures (ECCM) capabilities, are beginning to appear in the commercial sector. Specifically, spread-spectrum technology is being employed in digital cellular radio systems. These systems are identical to the military systems except that they employ much simpler spreading code design and have less security incorporated. However, due to the economies of scale, they can be produced at a much lower cost than their military counterparts.

The jamming vulnerability of such commercial products in tactical situations is analyzed in this thesis. The mobile cellular network developed by Qualcomm Inc. is used to illustrate the methodology in analyzing the effects of jamming on the mobile cellular network. With a single mobile station and jammer, the probability of jamming and the optimal jammer trajectory are derived. Next, the effective probabilities of detection and false alarm under the jamming conditions are derived and the mean acquisition times are compared to that without jamming. Our results show that intelligent jamming can cause devastating effects even with very small power. Commercial products are therefore much more vulnerable due to the simplicity in design.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENT

I am pleased to acknowledge the assistance of my thesis advisor Professor Alex W. Lam for his many helpful suggestions, ideas and guidance, and to my second reader Professor Donald v. Z. Wadsworth for his valuable comments.

I also wish to thank MINDEF for sponsoring my MSEE degree and thereby allowing me to have this opportunity to perform the research highlighted in this thesis.

Finally, I am grateful to my wife, Catherine and my daughters, Amy and Chloe for their moral support, patience and understanding during my entire course of study.

I. INTRODUCTION

A. GENERAL

Spread-spectrum is a modulation technique used for the transmission of digital signal in which the transmitted signal occupies a bandwidth in excess of the minimum necessary to send the information. The spreading of the signal is accomplished by means of a Pseudo-Noise (PN) code which is independent of the data. The despreading and subsequent data recovery at the receiver is accomplished by using a synchronized PN code.

There are three major types of spread-spectrum systems: Direct Sequence (DS), Frequency Hopping (FH) and Time Hopping (TH) systems. Hybrids of these systems have also been used.

B. DEVELOPMENT OF SPREAD-SPECTRUM

Spread-spectrum has a very long and interesting history [Ref. 1]. It has been used as a technique for the Electronic Counter Counter Measures (ECCM) in military communications systems since the mid-1950's. However, there are a few reasons which helped spread-spectrum gain popularity in commercial communications.

Firstly, with the imminent ending of the cold-war, the U.S. Government has decreased Department of Defence spending. This has affected the research and development and manufacturing of spread-spectrum products. Therefore, researchers and manufacturers of spread-spectrum products have started looking for alternate uses of spread-spectrum products.

Secondly, spread-spectrum techniques allow different users to share the already over crowded and limited radio spectrum. Spread-spectrum techniques by themselves provide very inefficient usage of the bandwidth because of the spreading process. However, the spreading allows different users to overlay the existing radio spectrum and therefore make efficient spectrum usage. It also allows the sharing of channels in the digital mobile cellular radio system which increases system capacity when compared to an analog system.

Last, but not least, in 1983 Federal Communications Commission (FCC) opened the Industrial, Scientific, and Medical (ISM) frequency band for unlicensed operation of devices under FCC technical regulations 15.247. This permits spread-spectrum modulation at a maximum transmitter power of 1 W in three bands - 902 to 928 MHz, 2400 to 2483.5 MHz, and 5725 to 5850 MHz. This, of course, allowed many small business ventures to start manufacturing and selling spread-spectrum products without obtaining licensing from FCC.

The ISM band has since been congested with thousands of spread-spectrum users. The FCC has in response opened other frequency bands for spread-spectrum users. From then on, spread-spectrum systems have found their way in many commercial systems such as Mobile Cellular Communications Systems, Personal Communications Network (PCN), Global Positioning System (GPS), Wireless Local Area Networks (WLAN) and many others.

C. COMMERCIAL SPREAD-SPECTRUM APPLICATIONS

1. Personal Communications Network

A PCN is a type of Personal Communications Services (PCS) that uses a cellular system which operates with cells placed about 1000 ft apart. The FCC has granted experimental license to a few spread-spectrum manufacturers to conduct field trials and studies in the 1850 to 1990 MHz band. This band is sparsely used for microwave transmission. Therefore, the idea is for the Code Division Multiple Access (CDMA) PCN system to share the same frequency band with existing microwave users and thereby increase the utilization efficiency of the frequency band.

The results of the field trials conducted by PCN America, Inc. in Houston, Texas and Orlando, Florida for 2 years have shown that the PCN spread-spectrum system can co-exist with those point-to-point microwave facilities operating at 1850 to 1990 MHz as long as the PCN systems are operating at data rates of T-1 (1.544 Mbps) or less. [Ref. 2] In the near future, there will very likely be PCN users sharing the same frequency band with microwave users.

2. Global Positioning System

GPS, one of the military application of spread-spectrum has since been made available for commercial usage. The GPS enables users to determine their position on or above the earth's surface to an accuracy of within 10 to 20 m by measuring their range to four GPS satellites whose position is accurately known. [Ref. 3]

3. Wireless Local Area Network

Another very sizable market for commercial spread-spectrum usage is in WLAN. There are presently many manufacturers of WLAN, however, not all of them use spread-spectrum technologies. One example of spread-spectrum WLAN is the Multipoint Airlink developed by Cylink. It uses the ISM band 902 to 928 MHz and therefore no licensing is required. It allows data speeds from 1.2 to 64 kbps for synchronous transmission and up to 19.2 kbps for asynchronous transmission. [Ref. 4]

4. Other Applications

Other spread-spectrum users include Western Multiplex Corp.'s T1 digital microwave radio known as Lynx Radio. It uses direct sequence spread-spectrum coding to transport a full T1 digital signal. Lynx operates at 1 W under the ISM frequency band. [Ref. 5]

Other present and future spread-spectrum applications include automated data collection, wireless Private Branch Exchange (PBX), wireless Integrated Services Digital Network (ISDN), digital stereo and a host of other applications.

D. OUTLINE

This thesis will study the effects of an intelligent jammer on a mobile cellular network similar to the one developed by Qualcomm Inc. In the next chapter, a brief introduction to the Qualcomm's system will be provided. The details can be found in the proposed wideband spread-spectrum standards developed by Qualcomm [Ref. 6].

In chapter III, the system model will be developed and the probability of jamming a mobile station in the cell will be derived. The optimal trajectory for the jammer is also derived. Chapter IV compares the performance of the mobile station with and without the jammer. In particular, the effective probability of detection, effective probability of false alarm and the mean acquisition time are derived. Finally, the concluding chapter provides a summary of the thesis and recommendations for further research.

II. THE QUALCOMM DIGITAL MOBILE CELLULAR RADIO SYSTEM

A. GENERAL

Qualcomm developed a prototype CDMA digital cellular system in Nov 89 and carried out extensive technical field trial in Feb 90. The Qualcomm system uses a transmission bandwidth of 10 MHz which is subdivided into roughly 8 wideband CDMA channels of 1.23 MHz each. The first CDMA channel occupies the band from 869.415 MHz to 870.645 MHz for the forward link (from base station to mobile station), with a center frequency of 870.030 MHz. The corresponding channel for the reverse link (from mobile station to base station) occupies the band from 824.415 MHz to 825.645 MHz, with a center frequency of 825.030 MHz. The reverse link is always 45 MHz below that of the forward link. All forward transmissions in a CDMA cellular system share the same bandwidth, however, all reverse transmissions share a different frequency band of 1.23 MHz.

B. REVERSE CDMA CHANNEL

The block diagram for the reverse CDMA channel is shown in Figure 2.1. The input data rate can have values from 1.2 kbps to 9.6 kbps. The data is convolutional encoded with a code rate of 1/3 and a constraint length of 9 for error detection and correction. The convolutional encoder used is shown in Figure 2.2. For each input bit to the convolutional encoder, three code symbols c_0, c_1, c_2 are generated at the output. Therefore, a 9.6 kbps data results in an output of 3x9.6 kbps or 28.8 ksps. As for data rates less than 9.6 kbps, the output will be repeated until the output is at a constant symbol rate of 28.8 ksps, i.e., a 2.4 kbps input will be repeated 3 times (each symbol occurs 4 times).

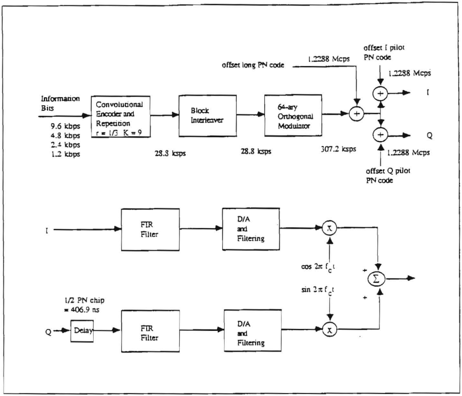


Figure 2.1 Transmitter for the reverse CDMA channel [Ref. 7].

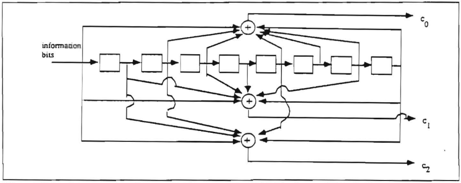


Figure 2.2 Convolutional encoder for reverse CDMA channel [Ref. 7].

The convolutional encoder is followed by the block interleaver. The purpose of interleaving is to disperse the effect of bursty channel errors since convolutional codes are effective in correcting non-bursty random channel errors. The encoded information is grouped into 6 symbol groups (or code words). These code words are used to select one of the 64 different orthogonal Walsh symbols or Hadamard codewords for transmission. Each Walsh symbol is a row of the Hadamard matrix. The Hadamard matrix H_{2m}, where m is a power of 2, is generated by the matrix in an iterative manner.

$$H_{2m}=\begin{bmatrix} H_m & H_m \\ H_m & \overline{H_m} \end{bmatrix} \tag{2.1}$$

with initial condition

$$H_2=\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \tag{2.2}$$

The Hadamard codewords are orthogonal. That is, the dot product of any two codeword is zero when the code bit 0 is transformed to 1 and the code bit 1 is transformed to -1. Since these codewords are orthogonal, they can be uniquely demodulated at the base station.

The orthogonal modulator output is spread by a long PN sequence with a period of 2^{42} -1. The long PN sequence is a m-sequence with 42 shift registers. All mobile stations in the CDMA system will use this same long PN sequence with a unique phase offset. The long PN sequence has a chip rate of 1.2288 Mcps. Since the Walsh chip rate is 307.2 kcps, each Walsh chip is spread by 4 long PN sequence chips.

The outgoing PN spread signal is further spread by 2 short PN sequences. They are the In-phase (I) and Quadrature-phase (Q) pilot PN sequences. They are called pilot PN sequences because the base station uses them to broadcast a quadriphase PN spread pilot synchronization signal. All transmissions in the CDMA system, either from mobile stations or base stations, share the same pair of pilot sequences. Different cells uses a different phase offset for the pilot PN codes, and all the transmissions within the same cell have the same pilot PN code phase offset. Signals from different cells are therefore distinguishable.

These short PN sequences are generated from m-sequences with period equal to $2^{15}-1$ = 32,767. However, for each period of the m-sequence, a 0 is inserted after a run of 14 0's, this increases the I and Q sequences to a period of 32,768. The total number of available phases, L is therefore 32,768. The time clock of the I and Q pilot PN sequence generators are at 1.2288 MHz, which is same as the long PN sequence time clock. The time period of the pilot PN sequence is equal to 32,768/1.2288 = 26.667 ms and therefore there are exactly 75 pilot PN sequence repetitions every 2 seconds.

After the long and short sequence spreading, the quadrature channel undergoes a delay of half a PN chip. This quadriphase spreading is called Offset Quadrature Phase shift keying (OQPSK). The OQPSK has the advantage of less abrupt phase changes and hence less distortion when amplified as compared to the QPSK. The I and Q channels are then bandlimited to 0.615 MHz by digital Finite Impulse Response (FIR) filters. The baseband signals are then modulated onto quadrature carriers, summed, amplified and then transmitted.

In summary, the reverse channel uses a 64 orthogonal data modulation with OQPSK PN spreading. The receiver at the base station attains frame and chip synchronization with the mobile station. However, the carrier phase is not synchronized and the demodulation at the base station is by non-coherent orthogonal demodulation. The phase offset of the long PN sequence gives a unique address to each mobile station while the short I and Q PN sequence gives a unique address to each cell.

C. FORWARD CDMA CHANNEL

The block diagram for the forward CDMA channel is shown in Figure 2.3. It comprises 64 code channels that are transmitted on a single 1.23 MHz forward CDMA bandwidth. The information goes through a convolutional encoder as shown in Figure 2.4 with a rate of 1/2 and constraint length 9. It is repeated just as in the case of the reverse channel if the data rate is less than 9.6 kbps. After encoding, it is block interleaved, biphase spread by the long PN sequence with a unique phase offset, biphase modulated by a Walsh function (which has 64 Walsh chips), quadriphase spread by the I and Q short pilot PN sequences. After that the quadrature channels are filtered and modulated onto quadrature channels and then transmitted.

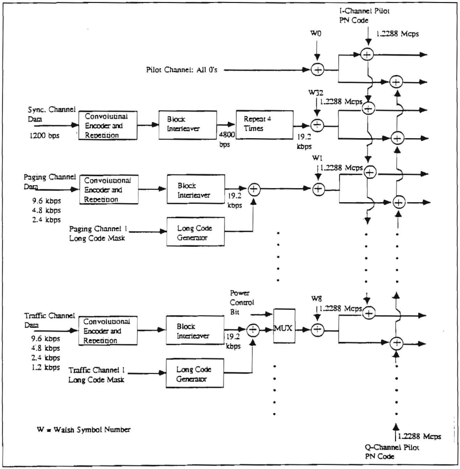


Figure 2.3 Transmitter for forward CDMA channel [Ref. 7].

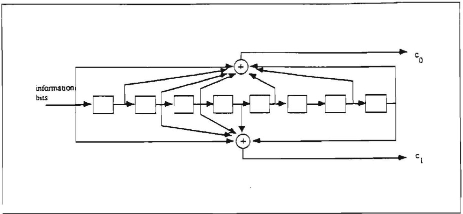


Figure 2.4 Convolutional encoder for forward CDMA channel [Ref. 7].

The spreading by the long PN sequence is a scrambling operation that provides data privacy for the mobile station. The 64 code channels are each specified by a Walsh function. The orthogonality among the 64 Walsh function provides nearly perfect isolation between the multiple signals transmitted by the base station, and these multiplexed signals are distinguishable at the mobile stations.

An important aspect of the forward link is the use of the pilot signal that is transmitted by each base station and is used as a coherent carrier reference for demodulation by all the mobile stations. The pilot is transmitted at a relatively higher level than other types of signals allowing extremely accurate tracking. The pilot channel signal is unmodulated by information and uses the zero Walsh function (which comprises 64 0's). Thus, the signal simply consists of the quadrature pair of PN codes. The mobile station can obtain synchronization with the nearest base station by searching out the entire length of the PN code. The strongest signal's time offset corresponds to time offset of the nearest base station's PN code. After synchronization, the pilot signal is used as a coherent carrier phase reference for demodulation of the other signals from this base station.

In the reverse CDMA channel, we have seen that the 64 Walsh functions are used to provide orthogonal data modulation. However, in the forward channel, the same Walsh functions are used to provide orthogonal covering of 64 code channels. The selection of the Walsh functions is determined by the mobile station's assigned code channel.

In summary, the forward channel uses coherent BPSK modulation with QPSK PN spreading. It transmits 64 orthogonal code channels in a frequency bandwidth of 1.23 MHz. The phase offsets in the short I and Q PN sequences will provide the identity of the base station. The phase offsets in the long PN code provides the identity of the mobile station. The pilot channel allows a mobile station to acquire the timing of the forward CDMA channels, provides a phase reference for coherent demodulation, and provides a reference for signal strength comparisons between base stations for determining when to hand-off.

D. PROCESSING GAIN OF THE SYSTEM

The processing gain of spread-spectrum system is an important performance parameter since it is a measure of how well the system can suppress interfering signals. It is commonly know as the spreading factor and is defined as

$$\begin{aligned} PG &= \frac{\text{Chip rate}}{\text{Data rate}} \\ &= \frac{R_c}{R_b}. \end{aligned} \tag{2.3}$$

For the Qualcomm CDMA system, the chip rate, R_c is 1.2288 MHz and the data rate, R_b varies from 1.2 kbps to 9.6 kbps. Therefore, the processing gain varies from 128 (21 dB) to 1024 (30 dB) depending on the data rate.

E. CAPACITY OF THE CDMA SYSTEM

In CDMA, frequency reuse efficiency is determined by the signal-to-interference ratio resulting from all the system users within range, not just those in any given cell. Since the total capacity becomes quite large, the statistics of the users are what is important, not any single user. This means that the net interference to any given signal is simply the average of all the users' received power times the number of users. As long as the ratio of the received signal power to the average noise power density is greater than a threshold value then the channel will provide an acceptable signal quality.

The primary parameters that determine the CDMA digital cellular system capacity are processing gain, the E_b/N_0 (with the required margin for fading), the voice duty cycle, the CDMA omni-directional frequency reuse efficiency, and the number of sectors in the cell-site antenna. The complete equation for determination of capacity in Qualcomm's CDMA system is as follows [Ref. 8]:

$$N=\frac{W}{R}\frac{1}{\frac{E_b}{N_0}}\frac{1}{d}\,F\,G. \tag{2.4}$$

where

N = Calls per cell (Assuming Rayleigh Fading reverse link)
W = Spread spectrum bandwidth (Assuming 1.2288 MHz)
R = Data rate (Assuming 9.6 kbps)
E_b/N_0 = Bit energy/noise power spectral density (Assuming 6.0 dB)
d = Voice duty cycle (Assuming 50%)
F = Frequency reuse efficiency (Assuming 60%)
G = Number of sectors in cell (Assuming 3 sectors)

Using the above equation with the assumed values of the parameters, we see that the CDMA system can support about 116 channels.

F. POWER CONTROL IN CDMA

In CDMA mobile cellular systems, it is very important to control the power of each mobile station such that the power received at the base station is nominal. If the received power is below nominal, then the bit error rate would increase and performance degrades. However, if the received signal power of a mobile station is above nominal, then the performance of that mobile station will be good but other mobile stations will suffer interference and their performance will degrade.

The Qualcomm reverse link power control uses both an open loop control as well as a closed loop control. In the open loop control, the mobile station estimates its minimum transmit power required to reach the base station based on the measurement of the received power of the pilot signal from the base station. However, since the forward and reverse link frequencies are separated by 45 MHz, the fading experienced by these two links are independent, the open loop control is not ideal. Therefore, on top of the open loop control, the mobile station also uses a closed loop control. In closed loop control, the base station measures the received signal strength from the mobile station and compares it to the desired signal strength and sends out power adjustment commands to the mobile station. This power adjustment command is combined with the mobile station's open loop estimate to obtain the final value of the mobile station's transmit power.

The forward link also employs a power control. In this case the base station adjusts its transmit power based on requests from mobile stations. The adjustment would usually be small and the base station must also consider the power demands being made on it by all the mobile stations in deciding whether to comply with the request of any particular mobile station.

III. SYSTEM MODEL AND PROBABILITY OF JAMMING

In this chapter, we shall study the effect of a jammer stationed within a single cell with one mobile station. We will derive the probability of jamming for the mobile station as a function of the ratio of the Effective Isotropic Radiated Power (EIRP) of the jammer and the base station as well as the relative distances between the base station, jammer and mobile station.

A. SYSTEM MODEL

Consider a single mobile station M, which can be uniformly distributed in a cell of normalized radius and with a base station B at the center. The base station has an antenna gain G_B, and a transmit power P_B while the mobile station has an antenna gain of G_M. Now consider an intelligent jammer which knows the I, Q sequences and their exact phases used by the base station for this cell. The jammer transmits a signal at a power of P_J and a gain of G_J with a different phase as the base station so as to confuse the mobile station. One possible disposition of the base station, mobile station and jammer is shown in Figure 3.1.

The received power at the mobile station from the base station P_{RB} is given by

$$P_{RB}=\frac{P_B G_B G_M \lambda^2}{(4\pi d_{BM})^2}, \tag{3.1}$$

where λ is the wavelength of the transmitted signal from base station to mobile station and d_{BM} is the distance from the base station to the mobile station.

The received power at the mobile station from the jammer P_{RJ} is similarly given by

$$P_{RJ}=\frac{P_J G_J G_M \lambda^2}{(4\pi d_{JM})^2}, \tag{3.2}$$

where d_{JM} is the distance from the jammer to the mobile station.

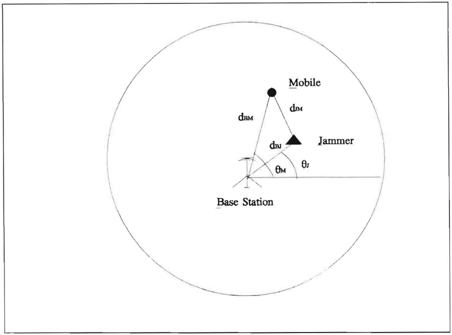


Figure 3.1 One possible disposition of the base station, mobile station and jammer.

From Figure 3.1 and using cosine rule, we can express d_{JM} as

$$d_{JM}=\sqrt{d_{BJ}^2+d_{BM}^2-2d_{BJ}d_{BM}\cos\left(\theta_M-\theta_J\right)}\ , \tag{3.3}$$

where d_{BJ} is the distance from the base station to the jammer and θ_M and θ_J are the angles as shown in Figure 3.1.

For jamming to be effective, that is when the mobile station locks-on to the jamming signal instead of the base station's signal, the received power from the jammer must be greater than the received power from the base station at the mobile station. When the two received powers are equal, we get

$$P_{RB}=P_{RJ},$$

$$\frac{P_B G_B G_M \lambda^2}{(4\pi d_{BM})^2}=\frac{P_J G_J G_M \lambda^2}{(4\pi d_{JM})^2}. \tag{3.4}$$

By simplifying and defining

$$P_t=\frac{P_J G_J}{P_B G_B}, \tag{3.5}$$

and

$$r=\frac{d_{BJ}}{d_{BM}}, \tag{3.6}$$

we can get

$$r^2-2r\cos(\theta_M-\theta_J)+1-P_t=0. \tag{3.7}$$

For simplicity of discussion we assume $\theta_J = \theta_M$, and we get,

$$r^2-2r+1-P_t=0. \tag{3.8}$$

By solving this quadratic equation, we get

$$r = 1\pm\sqrt{P_t}, \tag{3.9}$$

or

$$d_{BM} = \frac{d_{BJ}}{1\pm\sqrt{P_t}}. \tag{3.10}$$

The two locations of the mobile station where the power received from the base station and jammer are equal are as shown in Figure 3.2. By solving equation 3.7 for different values of θ_M, we can trace the loci of the points where the mobile station will receive equal power from the base station and jammer. The loci is a circle with center C and radius R where

$$C = \frac{d_{BJ}}{(1-P_t)}, \tag{3.11}$$

and

$$R = d_{BJ}\frac{\sqrt{P_t}}{(1-P_t)}. \tag{3.12}$$

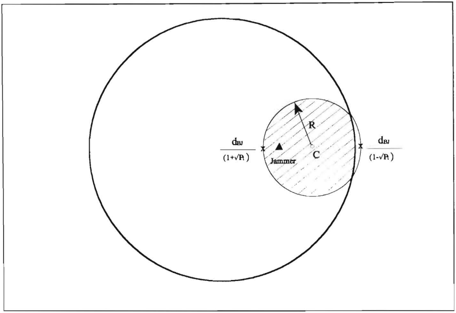

R
$\frac{d_{BJ}}{(1+\sqrt{P_t})}$
Jammer
C
$\frac{d_{BJ}}{(1-\sqrt{P_t})}$

Figure 3.2 The locations within the cell where the mobile station is jammed.

If the mobile station is on the circumference of this jamming circle, it receives equal power from the jammer as well as the base station. If the mobile station is within the shaded area of the jamming circle, it receives greater power from the jammer than the base station and is jammed. If the mobile station is within the unshaded area of the cell, it receives greater power from the base station than the jammer and is not jammed.

B. PROBABILITY OF JAMMING

The probability of the mobile station being jammed is the ratio of the shaded area to the total area of the cell and is a function of P_t and the location of the jammer. The location of the jammer which gives the maximum probability of jamming is known as the optimum jammer location d_{BJ}^*. So far, we have assumed that the jammer is stationary and the mobile station is uniformly distributed in the cell. However, in reality, the mobile station is not uniformly distributed and therefore, the jammer has to move to achieve the same probability of jamming. Since we have already found the optimum jammer location when the jammer is stationary, the optimal jammer trajectory is simply the loci of points joining the optimum jammer location when θ_J varies from 0 to 360°. This is simply a circle with the base station as the origin and the optimum jammer location as the radius. The optimum jammer location is shown in Figure 3.3 for different values of P_t.

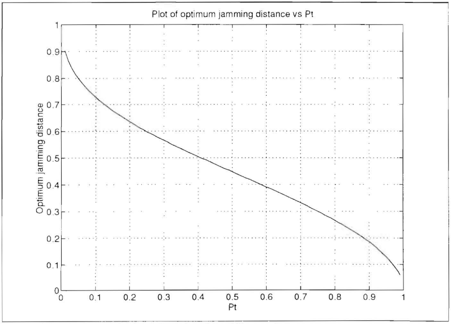


Figure 3.3 Optimum jammer location for different P_t.

Figure 3.3 shows that when P_t (the EIRP ratio of jammer to base station) is very small, the optimum jammer location d_{BJ}^* is far from the base station. When P_t increases, the optimum jammer location moves closer to the base station until when P_t is almost unity. In the limit, when $P_t = 0$, the jammer is at the circumference of the cell and when $P_t = 1$, the jammer is at the base station.

It is also interesting to study the variations on the center C and the radius R of the jamming circle to P_t. The center and the radius are functions of the location of the jammer. Note however, the center of the jamming circle is not the same as the optimum jammer location as shown in Figure 3.2. If we assume the jammer location is optimum, the variations of C and R are plotted in Figure 3.4 and 3.5 respectively.

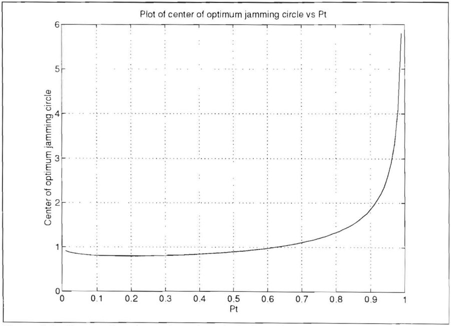


Figure 3.4 Center of optimum jamming circle for different P_t.

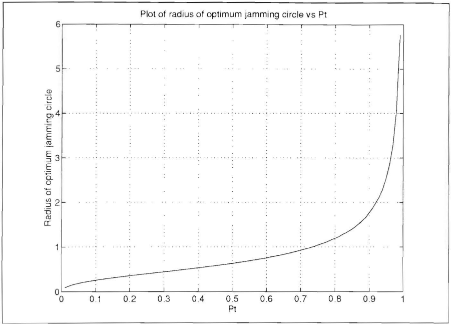


Figure 3.5 Radius of optimum jamming circle for different P_t.

From Figure 3.4, it is seen that when P_t is small, the center of the jamming circle is almost equal to unity and from Figure 3.5, the radius is almost zero. (i.e., there is no jamming at all). This means that a jammer with small power and omnidirectional antenna has a very small probability of jamming a mobile station in the cell. However, when P_t is almost unity, the center and radius of the jamming circle tends to infinity. (i.e., the jamming circle is half the cell). Although the jamming circle is only half of the cell, the interpretation is that a mobile station within the cell has 0.5 probability of being jammed.

Figures 3.3 to 3.5 shows that it is advantageous for a jammer with omnidirectional antenna to move closer to the base station when its power increases. The radius of its jamming circle also increases as the jammer moves closer to the base station. Figure 3.6 shows graphically the jamming circles for different P_t when the jammer is at the optimum location.

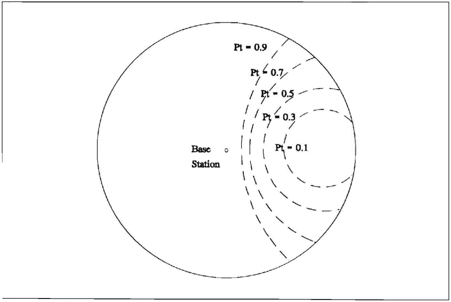


Figure 3.6 Jamming circles with different P_t.

The maximum probability of jamming for different values of P_t is obtained with an optimum position of the jammer and is plotted as shown in Figure 3.7.

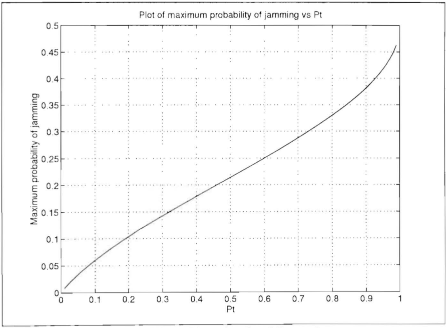
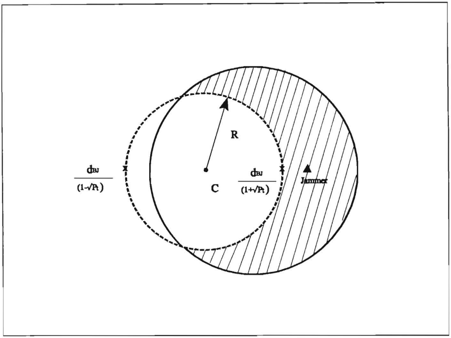


Figure 3.7 Maximum probability of jamming for different P_t.

It can be seen that when P_t is small, the probability of jamming is small. As P_t increases, the probability of jamming also increases. When P_t is unity, the probability of jamming is 0.5. This is because the mobile station receives equal power from the jammer and the base station and there is an equal chance that the mobile station will lock-on to either the base station or the jammer. However, when P_t is slightly greater than unity, the probability of jamming is unity since the mobile station will lock-on to the jammer instead of the base station. Therefore, there is a discontinuity in the probability of jamming when P_t is equal to unity.

From (3.10), when P_t is greater than unity, the locations within the cell where the mobile station is jammed is shown in Figure 3.8.



$\frac{d_{BJ}}{(1-\sqrt{P_t})}$
R
C
$\frac{d_{BJ}}{(1+\sqrt{P_t})}$
Jammer

Figure 3.8 Jamming area for P_t greater than unity.

From (3.11) and (3.12), it can be seen that when d_{BJ} is small, i.e., the jammer is close to the base station, the center, C and radius, R of the jamming circle is also small. In the limit when d_{BJ} is zero, i.e., the jammer is at the base station, the entire cell is jammed since C and R are both zero. Therefore, the optimal jamming distance, d_{BJ}^* for P_t greater than unity is always at the base station and this gives a probability of jamming of unity.

IV. PERFORMANCE ANALYSIS

In this chapter, we shall first derive the mean probability of detection and false alarm under no jamming based on noncoherent serial acquisition [Ref. 7] and then find the threshold that minimizes the mean acquisition time. Then by using this threshold, we shall derive the effective probability of detection and false alarm for the single user cell and single jammer. We shall also the find the deterioration in the mean acquisition time with a jammer with different power.

A. SYSTEM MODEL

The block diagram for a noncoherent serial scheme is as shown in Figure 4.1. In a serial acquisition scheme, the uncertainty phases are inspected one at a time, in a serial manner, until an aligned phase is found.

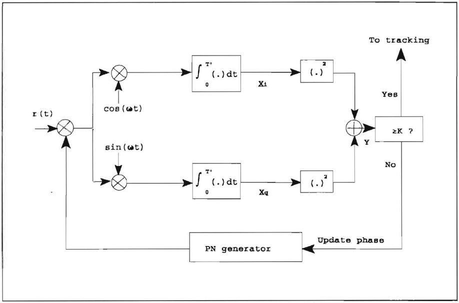


Figure 4.1 Block diagram of noncoherent serial acquisition scheme.

The input to the receiver r(t) comprises the base station's signal of power P_{RB}, additive white Gaussian noise with two-sided power spectral density of $N_o/2$ and jammer signal with power P_{RJ} Assuming that the jamming signal is wideband and centered around the center frequency of the base station, we model the jamming signal as white Gaussian noise with a one-sided power spectral density of $N_J = P_{RJ}T_b/2$ where P_{RJ} is the received power from the jammer and T_b is the bit period.

The probability of detection P_d is derived in [Ref. 7] and is given by

$$P_d = \int_K^\infty \frac{1}{2\sigma^2} e^{-(u+\lambda_1)/2\sigma^2} I_o\left(\frac{\sqrt{\lambda_1 u}}{\sigma^2}\right) du \tag{4.1}$$

where

$$\lambda_1 = \frac{P_{RB}T'^2}{2}\left[1 - \frac{|\gamma|}{T_c}\right]^2, \tag{4.2}$$

and

$$\sigma^2 = \left[\frac{N_o}{4} + \frac{N_J}{4}\right] T'. \tag{4.3}$$

P_{RB} is the received power from the base station, T' is the integration time, K is the threshold and $|\gamma| \le 0.5$ represents the misalignment of the incoming phase and the reference phase.

The probability of false alarm is given by

$$P_{fa} = \int_K^\infty \frac{1}{2\sigma^2} e^{-u/2\sigma^2} du = e^{-K/2\sigma^2}. \tag{4.4}$$

B. PERFORMANCE ANALYSIS WITH NO JAMMING

1. Probability of Detection and False Alarm

In order to calculate the probability of detection and probability of false alarm, we need to know the threshold, K in the receiver of the mobile station. We shall first examine the case without the jamming signal and determine the minimum mean acquisition time.

As we have found in the previous chapter, the power received from the base station by the mobile station depends on the location of the mobile station. Representing the location of the mobile station in cartesean coordinates (x, y), the power received from the base station can be represented as

$$P_{RB} = \frac{P_B G_B G_M \lambda^2}{(4\pi)^2 (x^2 + y^2)} . \tag{4.5}$$

As an example , let us assume that the base station and the mobile station have the following parameters.

Power of base station, P_B = 1 W

Gain of base station's antenna, G_B = 0 dB

Gain of mobile station's antenna, G_M = 0 dB

Wavelength, λ = 0.34 m (Frequency, f = 870 MHz)

Chip period, T_c = 1/1.2288 μs = 0.8138 μs

Bit period, T_b = 1/9600 s = 104.167 μs

One-sided noise power spectral density N_o = 4 x 10^{-21} W/Hz

Integration time T' = 1/9600 s = 104.167 μs

Misalignment, γ = 0.5 T_c

The probability of detection, P_d and probability of false alarm, P_{fa} for each mobile station's location (x, y) are calculated using (4.1) to (4.5) except that in (4.3), $N_j = 0$ since we assume the absence of the jamming signal. In this case, σ is calculated to be 3.2e-13. A mesh plot for the probability of detection and probability of false alarm with a threshold of K=1e-20 is shown in Figure 4.2 and 4.3 respectively.

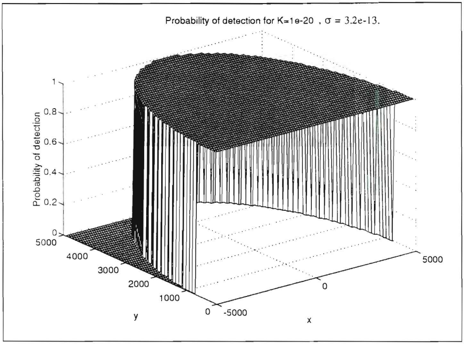


Figure 4.2 Plot of probability of detection with no jamming.

In Figure 4.2, we have divided half the cell with radius 5000 m into 800 points with the x axis from -5000 to 5000 and y axis from 0 to 5000. The probability of detection is calculated for each point. The lower half of the cell is symmetrical since we have assumed that the jammer is located along the x axis. Figure 4.2 shows that the probability of detection is almost unity within the entire cell.

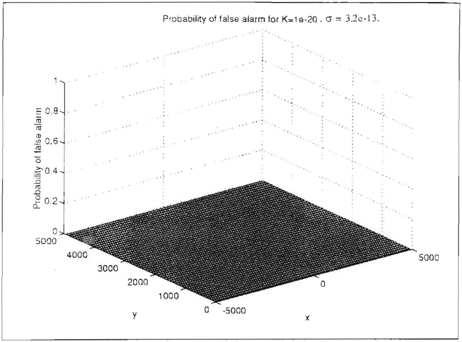


Figure 4.3 Plot of probability of false alarm with no jamming.

Figure 4.3 shows that the probability of false alarm is nearly zero within the entire cell for a threshold of 1e-20. Therefore, the threshold of 1e-20, gives a high probability of detection and low probability of false alarm. We shall confirm that this is indeed a good threshold by obtaining the threshold that minimizes the mean acquisition time.

Before we find the mean acquisition time, we need to define the mean probability of detection and false alarm as the sum of all the probabilities of detection and false alarm at all points within the cell divided by the number of points respectively.

The mean probabilities of detection and false alarm are plotted versus different thresholds in Figure 4.4 and 4.5 respectively.

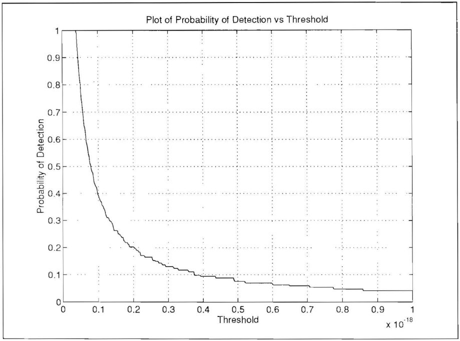


Figure 4.4 Plot of mean probability of detection for different thresholds.

Figure 4.4 shows that the mean probability of detection decreases when the threshold increases. This is by no means a surprise, since we know from (4.1) that the probability of detection is simply the portion of the area under the probability density function (pdf) where u is greater than the threshold K. The pdf approaches a normal distribution since the variance σ^2 is very small in this case. The portion of the area under the pdf gets smaller as K is increased.

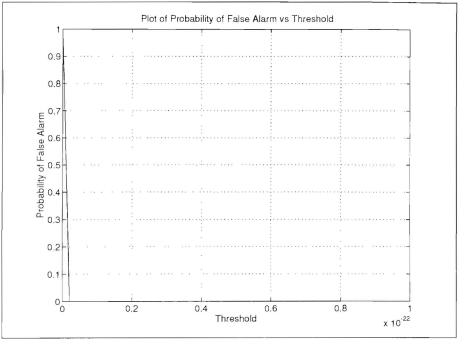


Figure 4.5 Plot of mean probability of false alarm for different thresholds.

Figure 4.5 shows that the probability of false alarm is nearly zero for all values except for very small values close to the noise power, σ^2. From (4.4), we notice that the probability of false alarm is independent of the signal and is solely dependent on the noise power. In this case, the noise power is very small, therefore, the probability of false alarm is nearly zero. Of course for values of K much smaller than σ^2, the probability of false alarm is no longer negligible.

2. Mean Acquisition Time

From [Ref. 7], the mean acquisition time T_{acq} is related to P_d, and P_{fa} as in (4.6).

$$T_{acq} = L\frac{(1-0.5P_d)}{P_d}\left[T' + \frac{P_{fa}}{(1-P_{fa})^2}T_p\right], \tag{4.6}$$

where L is the total number of different phases in the I, Q PN sequence and T_p is the penalty time incurred for each false alarm.

The mean acquisition time is the parameter that we shall strive to minimize. This can be done by varying the threshold and the integration time. By assuming an integration time, T' of T_b, and using a penalty time of 10 x T_b and L = 32768, we can plot the mean acquisition time using (4.6) in Figure 4.6.

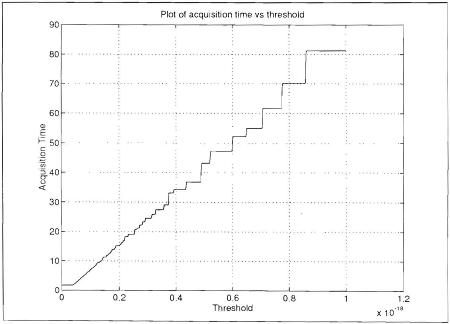


Figure 4.6 Mean acquisition time for different thresholds with T_p = $10T_b$.

We can see from Figure 4.6 that the threshold which gives the minimum mean acquisition time lies between 0 and 1e-19. By enlarging the plot in the region of interest as shown in Figure 4.7, we see that the threshold is around 1e-20. This gives a mean acquisition time of 1.7 s which is very near to the value given in [Ref. 6]. According to [Ref. 6], the mean acquisition time should be less than 2 s.

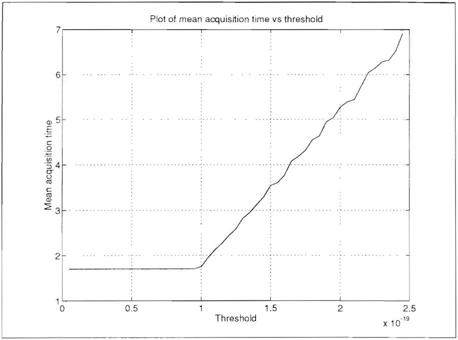


Figure 4.7 Enlarged plot of mean acquisition time for different thresholds with $T_p=10T_b$.

We shall now use the threshold of 1e-20 for the analysis in the performance under jamming.

C. PERFORMANCE ANALYSIS WITH JAMMING

For the case of a mobile station in a cell with a jammer as shown in Figure 4.8, the mobile station can be either within the jamming circle (in shaded region) or outside the jamming circle (in the unshaded region of the cell).

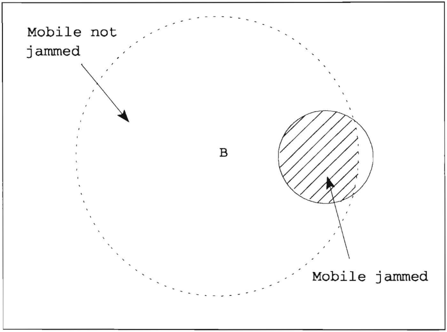


Figure 4.8 Mobile station in a cell with a jammer.

With the assumption of an intelligent jammer that transmits the same bandwidth as the base station's signal, with the same PN sequence but at a different phase, the mobile station will lock-on to the jammer if it's inside the jamming circle, and lock-on to the base station if it's outside the jamming circle.

1. Effective Probability of Detection and False Alarm

The effective probability of detection, $P_{d,eff}$ is derived using the total probability. Since the probability of detection when the mobile station is within the jamming circle is 0, the effective probability of detection is simply the product of the probability of the mobile station not being jammed and the conditional probability of detection given that the mobile station is not jammed as given by

$$\begin{aligned} P_{d,eff} &= Pr(jammed)\,xP_d(jammed) + Pr(\overline{jammed})\,xP_d(\overline{jammed}) \\ &= Pr(jammed)\,x0 + Pr(\overline{jammed})\,xP_d(\overline{jammed}) \\ &= Pr(\overline{jammed})\,xP_d(\overline{jammed})\;. \end{aligned} \tag{4.7}$$

The effective probability of false alarm, $P_{fa,eff}$ can also be derived using the total probability. The probability of false alarm given that the mobile station is not jammed is simply calculated by (4.4). The probability of false alarm given that the mobile station is jammed is the sum of the probability of detecting the phase of the jamming signal and the probability of detecting a phase which belongs to neither the base station nor the jammer. The latter probability is just the probability of false alarm for the jamming signal multiplied by the factor $(L\text{-}2)/(L\text{-}1)$. Since L is usually large, this factor approximates to one. The probability of false alarm on the jamming signal when the mobile station is jammed is usually very small and the probability of detecting the jamming signal when the mobile station is jammed is usually very near unity. Therefore, to simplify the analysis, we assume that the sum of the probability of detection and probability of the false alarm on the jamming signal is approximately one, then $P_{fa,eff}$ approximates to the product of the probability of the mobile station not being jammed and probability of false alarm given that the mobile station is not jammed plus the probability that the mobile station is jammed as

$$
\begin{aligned}
P_{fa,eff} &= Pr(\overline{jammed})\,xP_{fa}(\overline{jammed}) + \\
&\quad Pr(jammed)\,x[P_d(jammed) + P_{fa}(jammed)\,x\frac{L-2}{L-1}] \\
&\approx Pr(\overline{jammed})\,xP_{fa}(\overline{jammed}) + Pr(jammed)\,.
\end{aligned}
\tag{4.8}
$$

Now, just as in the previous section, the power received from the jammer by the mobile station depends on the location of the mobile station and can be represented as

$$
P_{RJ} = \frac{P_J G_J G_M \lambda^2}{(4\pi)^2[d_{BJ}^2 + x^2 + y^2 - 2d_{BJ}\sqrt{x^2+y^2}\cos(\tan^{-1}\frac{y}{x})]}\,, \tag{4.9a}
$$

when x ≥ 0 and,

$$
P_{RJ} = \frac{P_J G_J G_M \lambda^2}{(4\pi)^2[d_{BJ}^2 + x^2 + y^2 + 2d_{BJ}\sqrt{x^2+y^2}\cos(\tan^{-1}\frac{y}{x})]}\,, \tag{4.9b}
$$

when x < 0.

As in the example in the previous section, let us assume the jammer is at its optimum location and with a power , P_J = 0.5 W and antenna gain, G_J = 0 dB. From Figure 3.3, we see that with P_t = 0.5, the optimum location of the jammer, d_{BJ} is 0.45.

The probability of detection, $P_{d,eff}$ and probability of false alarm, $P_{fa,eff}$ with the threshold set at 1e-20 is shown in Figure 4.9 and 4.10 respectively.

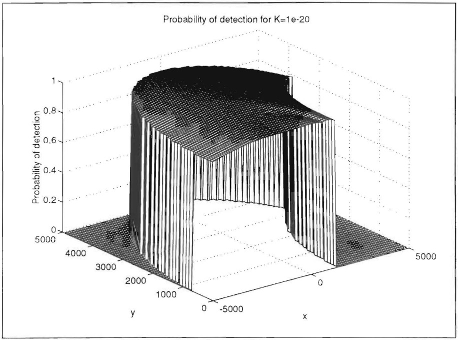


Figure 4.9 Plot of probability of detection with P_f = 0.5.

Comparing Figures 4.2 and 4.9, we see that the jammer has reduced the probability of detection. The probability of detection near the origin is higher since it is nearer to the base station and receives a stronger signal from the base station. However, the further the mobile station is from the base station, the lower is the probability of detection. This is due to the effect of the jammer. It is especially significant along the x axis where the jammer is located. The probability of detection within the jamming circle is zero since we have assumed that the mobile station will lock-on to the jamming signal and hence will not detect the base station's signal.

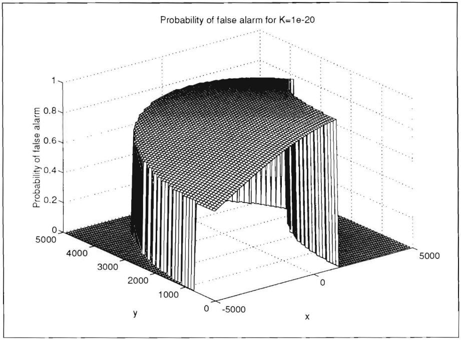


Figure 4.10 Plot of probability of false alarm with P_t = 0.5.

Comparing Figure 4.3 and 4.10, we see that the false alarm is no longer zero. This is because of the noise created by the jammer has a significant effect on the probability of false alarm. Points nearer to the jammer suffer a higher probability of false alarm. The probability of false alarm becomes smaller as we move further from the jammer. The probability of false alarm within the jamming circle is not defined since the mobile station will lock-on to the jamming signal.

Similar to the previous section, we take the mean probabilities by adding the probabilities for all points within the cell but outside the jamming circle and then dividing it by the number of points. These mean probabilities are the mean conditional probability of detection and the mean conditional probability of false alarm given that the mobile station is not jammed. Using (4.7) and (4.8), and from Figure 3.7, the probability of jamming for P_t = 0.5 is 0.21, we can calculate and plot the effective probability of detection and false alarm as shown in Figure 4.11 and 4.12 respectively.

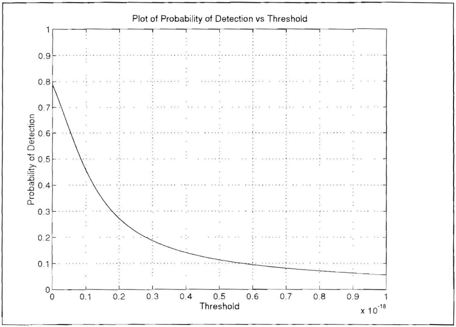


Figure 4.11 Plot of effective probability of detection for different thresholds, P_t = 0.5.

From Figure 4.11, we see that the maximum $P_{d,eff}$ is only 0.79 which is the probability of the mobile station not being jammed. Therefore, the maximum effective probability of detection is no longer one as in the case without jamming. The jammer has in fact reduced the effective probability of detection.

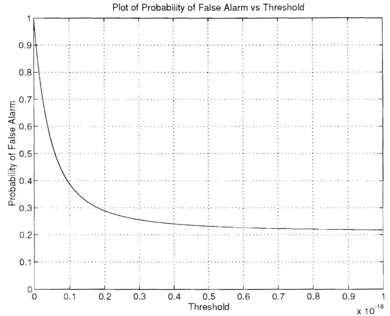


Figure 4.12 Plot of effective probability of false alarm for different thresholds, $P_t = 0.5$.

Similarly, from Figure 4.12, we see that the lower bound for $P_{fa,eff}$ is 0.21 and this is the probability of the mobile station being jammed as seen in (4.8). This implies that irrespective of the threshold value, the minimum effective probability of false alarm due to the jammer is 0.21. The jammer has also increased the effective probability of false alarm.

2. Mean Acquisition Time

Similar to the case of no jamming as highlighted in the previous section, the mean acquisition time T_{acq} where jamming is present is related to $P_{d,eff}$ and $P_{fa,eff}$ as

$$T_{acq} = L\frac{(1-0.5P_{d,eff})}{P_{d,eff}}\left[T' + \frac{P_{fa,eff}}{(1-P_{fa,eff})^2}T_p\right], \qquad (4.10)$$

where L is the total number of different phases in the I, Q PN sequence and T_p is the penalty time incurred for each false alarm. By assuming a penalty time of 10 x T_b and L = 32768, we can plot the mean acquisition time using (4.10) in Figure 4.13.

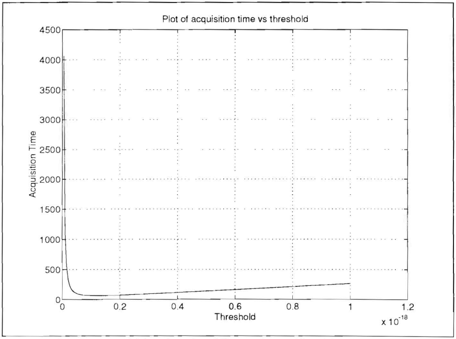


Figure 4.13 Mean acquisition time for different thresholds with P_t = 0.5 & T_p = $10T_b$.

From Figure 4.13, we find that the mean acquisition time at the threshold of 1e-20 is of the order of a thousand seconds. This clearly is not acceptable for all practical purposes. In other words, the jammer has effectively jammed the pilot signal and prevented the mobile station from locking-on to the base station's signal.

By enlarging Figure 4.13, we see from Figure 4.14 that the minimum mean acquisition time is now achieved at a threshold 1.2 e-19 and is around 63 s.

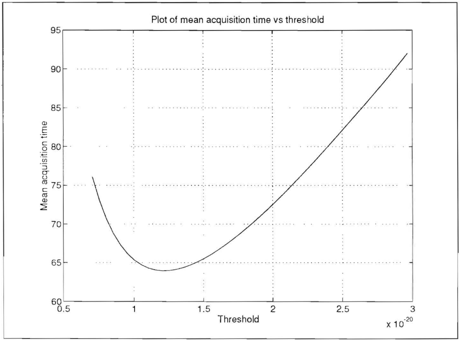


Figure 4.14 Enlarged plot of mean acquisition time for different thresholds with P_t = 0.5 & T_p= $10T_b$.

We will now examine the effect of varying the jamming power on the mean acquisition time. The mean acquisition time for three different P_t are shown in Figure 4.15.

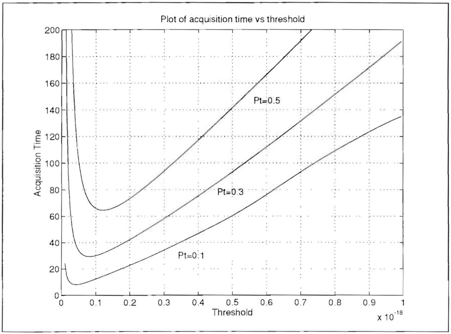


Figure 4.15 Mean acquisition time vs thresholds with different P_t, $T_p = 10T_b$.

Figure 4.15 shows that the power of the jammer does have a significant effect on the mean acquisition time. For example, an increase in P_t from 0.1 to 0.5 causes the mean acquisition time to increase from 8.13 s to 63 s.

Next, the effect of varying the penalty time, T_p on the mean acquisition time is studied. The mean acquisition time for three different penalty times are shown in Figure 4.16.

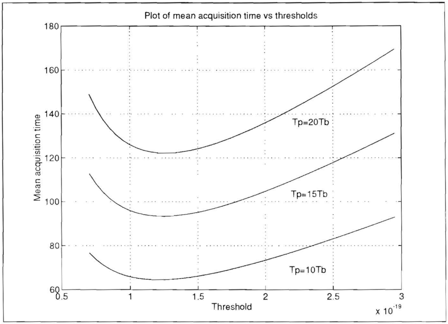


Figure 4.16 Mean acquisition time vs threshold with different T_p, P_t = 0.5.

From Figure 4.16, it can be seen that the penalty time also has a significant effect on the mean acquisition time. A doubling of penalty time, T_p from $10T_b$ to $20T_b$, causes approximately a doubling in the mean acquisition time from 63 s to 122 s.

V. CONCLUSIONS

A. SUMMARY

In this thesis, we have studied the effects of an intelligent jamming on a digital mobile cellular network similar to the one developed by Qualcomm Inc. The Qualcomm mobile cellular network uses CDMA technology. It supports data rates from 1.2 kbps to 9.6 kbps and has a processing gain of 21 dB to 30 dB depending on the data rate. For synchronization, the base station transmits an unmodulated pilot signal with two short In-phase, I and Quadrature phase, Q PN sequences which all the mobile stations try to acquire. Once the pilot signal is acquired, the mobile station knows the exact phase of the I and Q PN sequences used by the base station. It uses this information for coherent demodulation of subsequent data transmitted from the base station.

The probability that a mobile station within the cell is jammed was determined. By varying the position of the jammer within the cell, the probability of jamming varies. As expected, our results indicate that the probability of jamming depends on the power of the jammer as well as the position of the jammer. The locus of optimum locations which give the maximum probability of jamming for different powers is obtained. In general, for maximum probability of jamming, the higher the jamming power, the closer the jammer is to the base station.

We have also analyzed the effects of an intelligent jammer on the probability of detection, the probability of false alarm and the mean acquisition time for the mobile station to acquire the pilot signal of the base station. An intelligent jammer is one which transmits on the same bandwidth as the base station's signal, with the same PN sequence but at a different phase. By first ignoring the jamming signal, we derived the mobile station's threshold which minimizes the mean acquisition time. We have found that the minimum acquisition time is around 1.7 s which is very near to the 2 s value claimed by Qualcomm. With this threshold, we analyzed the probability of detection, probability of false alarm and the mean acquisition time in the presence of the jamming signal. We have found a significant increase in the mean acquisition time under jamming. For an intelligent jammer which transmits at 10% power of the base station, the mean acquisition time is increased from 1.7 s to 8.13 s, a five-fold increase. Our results indicate that it takes only a relatively low-powered intelligent jammer to render the network in-operative. The effects of the penalty time were also investigated.

B. RECOMMENDATIONS FOR FURTHER RESEARCH

1. Sensitivity of Mean Acquisition Time to Integration Time

In the thesis, we have seen the effects of false alarm penalty time on the mean acquisition time. It would be of interest to find out the effects of varying the integration time on the mean acquisition time.

2. Multiple Jammers

The results obtained in this thesis can be extended to the case of multiple jammers within the cell. This of course will increase the probability of jamming and provide even greater degradation to the mobile cellular network. With a suitable number of jammers, the power of each jammer can be reduced, thereby making it more difficult to locate the jammers. We should be able to find the optimum number of jammers with a certain power and their locations that will deliver the maximum degradation to the network.

3. Multiple Mobile Stations

In this thesis, we have considered only a single mobile station within the cell. Our results can be extended to multiple mobile stations. By assuming the mobile stations are distributed independently, we can find the probability jamming multiple mobile stations using the binomial distribution.

APPENDIX A. PROGRAMS TO CALCULATE AND PLOT OPTIMUM JAMMER LOCATION, CENTER OF JAMMING CIRCLE, RADIUS OF JAMMING CIRCLE AND PROBABILITY OF JAMMING

```
%*********************************************************************************%
%Program: probj.m                                                                  %
%                                                                                  %
%Calculates the optimum jammer location with different jamming power              %
%                                                                                  %
%Author: Eugene Chang                                                              %
%                                                                                  %
%Last Update: 4 Nov 94                                                             %
%                                                                                  %
%*********************************************************************************%
rc=1;                                   %Normalized radius of cell
k=1;                                    %Counter for pt
for pt=0.01:0.01:0.99                   %EIRP ratio pt
  i=1;                                  %Counter for Rj
  max_jamming_area=0;
  ro=rc*sqrt(pt)/(1-pt);
  for Rj=0.01:0.002:1                   %Jammer distance Rj
    R=Rj*ro;                            %Radius of jamming circle
    C=Rj /(1-pt);                       %Center of jamming circle
    if C+R <= rc                        %Jamming circle smaller than cell
      jamming_area(i)=pi*R .^2;
    else
      theta1=acos((1+C^2 - R^2) /(2*C));
      theta2=acos((R^2 +C ^2 -1) /(2*R*C));
      if imag(theta1) == 0 & imag(theta2) == 0
        jamming_area(i)=R.^2*theta2 + 0.5* sqrt(R .^2-0.5+0.5*cos(2*theta1))*sqrt(2-2*cos(2*theta1))
+theta1-0.5*sqrt(2-2*cos(2*theta1))*(C+ sqrt(R .^2-0.5+0.5*cos(2*theta1)));
      end
    end
    if jamming_area(i)>max_jamming_area
      max_jamming_area=jamming_area(i);
      optimum_jammer_distance(k)=Rj;
    end
    i=i+1;
  end
  max_prob_jamming(k)=max_jamming_area/pi;
  center_optimum(k)=optimum_jammer_distance(k)/(1-pt);  %Center for optimum jamming circle
  radius_optimum(k)=optimum_jammer_distance(k)*ro;      %Radius for optimum jamming circle
  k=k+1;
end
save probj
```

```
%*************************************************************************************%
%Program: plot_probj.m                                                                %
%                                                                                     %
%Plots the optimum jammer location with different jamming power                       %
%                                                                                     %
%Author: Eugene Chang                                                                 %
%                                                                                     %
%Last Update: 24 Oct 94                                                               %
%                                                                                     %
%*************************************************************************************%
%Plots the Optimum jammer location vs different jamming power                         %
%*************************************************************************************%
clear
load probj
figure (1)
clg
plot([0.01:0.01:0.99],optimum_jammer_distance);grid
title('Plot of optimum jammer radius Rj vs Pt')
xlabel('Pt')
ylabel('Optimum jammer location Rj')
%*************************************************************************************%
%Plots the center of optimum jamming circle vs Pt                                     %
%*************************************************************************************%
figure (2)
clg
plot([0.01:0.01:0.99], center_optimum);grid
title('Plot of center of optimum jamming circle vs Pt')
xlabel('Pt')
ylabel('Center of optimum jamming circle')
%*************************************************************************************%
%Plots the radius of optimum jamming circle vs Pt                                     %
%*************************************************************************************%
figure (3)
clg
plot([0.01:0.01:0.99], radius_optimum);grid
title('Plot of radius of optimum jamming circle vs Pt')
xlabel('Pt')
ylabel('Radius of optimum jamming circle')
%*************************************************************************************%
%Plots the Probability of jamming vs different Pt                                     %
%*************************************************************************************%
figure (4)
clg
plot([0.01:0.01:0.99],max_prob_jamming);grid
title('Plot of probability of jamming vs Pt')
xlabel('Pt')
ylabel('Probability of jamming')
```

APPENDIX B. PROGRAMS TO CALCULATE AND PLOT PROBABILITY OF DETECTION, PROBABILITY OF FALSE ALARM AND MEAN ACQUISITION TIME WITHOUT JAMMING

```
%*********************************************************************************%
%Program: pd0.m                                                                   %
%                                                                                 %
%Calculates probability of detection and false alarm with no jamming              %
%                                                                                 %
%Author: Eugene Chang                                                             %
%                                                                                 %
%Last Update: 18 Nov 94                                                           %
%                                                                                 %
%*********************************************************************************%
clear
PB=1;                          %Power of base = 1W
GB=1;                          %Gain of base = 1
GM=1;                          %Gain of mobile = 1
rc=5000;                       %Radius of cell
lamda=0.34;                    %Wavelength = 0.34m
Tc=8.138e-7;                   %Period of Spreading waveform
gamma=0.5*Tc;                  %Misalignment = 0.5
Tb=1/9600;                     %Bit period
T=Tb;                          %Integration time
No=4e-21;                      %Thermal noise
step_size=0.1*rc;              %Number of samples
k=1;
for K=0:5e-22:1e-19            %Threshold
  j=1;
  number_of_samples=0;
  Pd_y_x=[];
  Pfa_y_x=[];
  y_range=step_size/2:step_size:rc-step_size/2;
  x_range=-rc+step_size/2:step_size:rc-step_size/2;
  for y=y_range
     i=1;
     for x=x_range
         if sqrt(x^2 + y^2) <= rc
            number_of_samples=number_of_samples+1;
          PRB=PB*GB*GM*lamda^2 /((4*pi)^2*(x^2+y^2));
          lamda_1=PRB * T^2 /2 * (1 - gamma /Tc)^2;
          sigma2= No/4*T;
          Pd_y_x(i,j)= quad8('pdf',K,lamda_1*1.1,[],[],lamda_1,sigma2);
          Pfa_y_x(i,j)=exp(-K/(2*sigma2));
        else
          Pd_y_x(i,j)=0;
          Pfa_y_x(i,j)=0;
        end
        i=i+1;
```

```
      end
      j=j+1;
   end
   Pd(k)=sum(sum(Pd_y_x))/number_of_samples;
   Pfa(k)=sum(sum(Pfa_y_x))/number_of_samples;
   k=k+1;
end
save pd0

%*******************************************************************************%
%Program: plotj0.m                                                              %
%                                                                               %
%Plots the  probability of detection and false alarm without jamming            %
%                                                                               %
%Author: Eugene Chang                                                           %
%                                                                               %
%Last Update: 16 Nov 94                                                         %
%                                                                               %
%*******************************************************************************%
clear
load pd0
figure(1)
plot(0:5e-22:1e-19,Pd);grid
title('Plot of Probability of Detection vs Threshold')
xlabel('Threshold')
ylabel('Probability of Detection')
axis([0 1e-19 0 1]);
figure(2)
plot(0:5e-22:1e-19,Pfa);grid
title('Plot of Probability of False Alarm vs Threshold')
xlabel('Threshold')
ylabel('Probability of False Alarm')
axis([0 1e-19 0 1])

%*******************************************************************************%
%Program: tacq0.m                                                               %
%                                                                               %
%Plots the mean acquisition time without jamming                                %
%                                                                               %
%Author: Eugene Chang                                                           %
%                                                                               %
%Last Update: 15 Nov 94                                                         %
%                                                                               %
%*******************************************************************************%
clear
load pd0
Tp=10*Tb;                          %Penalty time
L=32768;                           %Number of phases
Tacq=L*(1-0.5*Pd) ./Pd .*(T+ Pfa ./(1-Pfa) .^2 *Tp);
plot(0:5e-22:1e-19,Tacq);grid
```

```
title('Plot of acquisition time vs threshold')
xlabel('Threshold')
ylabel('Acquisition Time')
```

APPENDIX. C PROGRAMS TO CALCULATE AND PLOT PROBABILITY OF DETECTION, PROBABILITY OF FALSE ALARM AND MEAN ACQUISITION TIME WITH JAMMING

```
%*************************************************************************************%
%Program: pd1.m                                                                       %
%                                                                                     %
%Calculates probability of detection and false alarm with jammer                      %
%                                                                                     %
%Author: Eugene Chang                                                                 %
%                                                                                     %
%Last Update: 17 Nov 94                                                               %
%                                                                                     %
%*************************************************************************************%
clear
PB=1;                   %Power of base = 1W
PJ=0.5;                 %Power of jammer =0.5W
GB=1;                   %Gain of base = 1
GJ=1;                   %Gain of jammer = 1
GM=1;                   %Gain of mobile = 1
rc=5000;                %Radius of cell
Rj=0.4480*rc;           %Optimum location of jammer
pt=(PJ*GJ)/(PB*GB);     %EIRP ratio
rj=Rj*sqrt(pt)/(1-pt);  %Radius of jamming circle
c=Rj/(1-pt);            %Center of jamming circle
lamda=0.34;             %Wavelength = 0.34m
Tc=8.138e-7;            %Period of Spreading waveform
gamma=0.5*Tc;           %Misalignment = 0.5
Tb=1/9600;              %Bit period
T=Tb;                   %Integration time
No=4e-21;               %Thermal noise
step_size=0.1*rc;       %Number of samples
k=1;
for K=0:5e-21:1e-18     %Threshold
  j=1;
  number_of_samples=0;
  Pd_y_x=[];
  Pfa_y_x=[];
  y_range=step_size/2:step_size:rc-step_size/2;
  x_range=-rc+step_size/2:step_size:rc-step_size/2;
  for y=y_range
     i=1;
     for x=x_range
         if sqrt((x-c)^2+ y^2) > rj & sqrt(x^2 + y^2) <= rc
            number_of_samples=number_of_samples+1;
          PRB=PB*GB*GM*lamda^2 /((4*pi)^2*(x^2+y^2));
          lamda_1=PRB * T^2 /2 * (1 - gamma /Tc)^2;
          if x > 0
             angle=atan(y/x);
```

```
        else
          angle=pi+atan(y/x);
        end
          d_jm2=Rj^2+x^2+y^2-2*Rj *sqrt(x^2+y^2)*cos(angle);
          PRJ=PJ*GJ*GM*lamda^2/((4*pi)^2* d_jm2);
          NJ=PRJ*Tb/2;
          sigma2=(No/4 + NJ/4)*T;
        maxp=quad8('pdf',0,lamda_1*10,[],[],lamda_1,sigma2);
        Pd_y_x(i,j) = quad8('pdf',K,lamda_1*10,[],[],lamda_1,sigma2)/maxp;
        Pfa_y_x(i,j)=exp(-K/(2*sigma2));
      else
        Pd_y_x(i,j)=0;
        Pfa_y_x(i,j)=0;
      end
      i=i+1;
    end
    j=j+1;
  end
  Pd(k)=sum(sum(Pd_y_x))/number_of_samples;
  Pfa(k)=sum(sum(Pfa_y_x))/number_of_samples;
  k=k+1;
end
save pd1

%*************************************************************************************%
%Program: plotj.m                                                                     %
%                                                                                     %
%Plots the  probability of detection and false alarm                                  %
%                                                                                     %
%Author: Eugene Chang                                                                 %
%                                                                                     %
%Last Update: 15 Nov 94                                                               %
%                                                                                     %
%*************************************************************************************%
clear
load pd1
p=0.2140;                      %Probability of jamming
figure(1)
plot(0:5e-21:1e-18,Pd*(1-p));grid
title('Plot of Probability of Detection vs Threshold')
xlabel('Threshold')
ylabel('Probability of Detection')
axis([0 1e-18 0 1]);
figure(2)
plot(0:5e-21:1e-18,Pfa*(1-p)+p);grid
title('Plot of Probability of False Alarm vs Threshold')
xlabel('Threshold')
ylabel('Probability of False Alarm')
axis([0 1e-18 0 1])
```

```
%****************************************************************************************%
%Program: tacq.m                                                                         %
%                                                                                        %
%Plots the mean acquisition time                                                         %
%                                                                                        %
%Author: Eugene Chang                                                                    %
%                                                                                        %
%Last Update: 15 Nov 94                                                                  %
%                                                                                        %
%****************************************************************************************%
clear
load pd1
Tp=10*Tb;                          %Penalty time
L=32768;                           %Number of phases
p=0.2140;                          %Probability of jamming
Pd_eff=(1-p)*Pd;                   %Effective probability of detection
Pfa_eff=(1-p)*Pfa + p;             %Effective probability of false alarm
Tacq=L*(1-0.5*Pd_eff) ./Pd_eff .*(T+ Pfa_eff ./(1-Pfa_eff) .^2 *Tp);
xaxis=0:5e-21:1e-18;
plot(xaxis(3:200),Tacq(3:200));grid
title('Plot of acquisition time vs threshold')
xlabel('Threshold')
ylabel('Acquisition Time')
```

APPENDIX D. MISCELLANEOUS PROGRAMS

```
%*************************************************************************%
%Program: mesh_plot.m                                                     %
%                                                                         %
%Plots the probability of detection and false alarm                       %
%                                                                         %
%Author: Eugene Chang                                                     %
%                                                                         %
%Last Update: 12 Nov 94                                                   %
%                                                                         %
%*************************************************************************%
figure(1)
mesh(x_range,y_range,Pd_y_x');grid
colormap([0 0 0])
title('Probability of detection for K=1e-20')
xlabel('x')
ylabel('y')
zlabel('Probability of detection')
axis([-rc rc 0 rc 0 1])
figure(2)
mesh(x_range,y_range,Pfa_y_x');grid
colormap([0 0 0])
title('Probability of false alarm for K=1e-20')
xlabel('x')
ylabel('y')
zlabel('Probability of false alarm')
axis([-rc rc 0 rc 0 1])
```

```
%*************************************************************************%
%Program: pdf.m                                                           %
%                                                                         %
%Calculates the probability density function                              %
%                                                                         %
%Author: Eugene Chang                                                     %
%                                                                         %
%Last Update: 12 Nov 94                                                   %
%                                                                         %
%*************************************************************************%
function y=pdf(u,lamda_1,sigma2)
for k=1:length(u)
  d(k)=sqrt(lamda_1*u(k))/sigma2;
  if d(k) < 10
    b(k)=besseli(0,d(k));
    a(k)=0.5*exp(0.5*(-u(k)-lamda_1/sigma2))/sigma2;
  else
    a(k)=1 ./sqrt(8*pi*sigma2*sqrt(u(k)*lamda_1));
    b(k)=exp(d(k)-0.5*(u(k)+lamda_1)/sigma2);
  end
  y(k)=a(k) * b(k);
end
```

LIST OF REFERENCES

1. Scholtz R. A., "The Origins of Spread-Spectrum Communications," *IEEE Transactions on Communications*, vol. 30, pp. 822-854, May 1982.

2. Milstein L. B., Schilling D. L., and et al., "On the Feasibility of a CDMA Overlay for Personal Communications Networks," *IEEE Journal on Selected Areas in Communications*, vol. 10, May 1992.

3. Getting, I. A., "The Global Positioning System," *IEEE Spectrum*, vol. 30, pp. 36-47, Dec. 1993.

4. Cylink, "Airlink Multipoint 64MP specifications," Cylink, 310N. Mary Avenue, Sunnyvale, CA 94086.

5. Schneiderman R., "Spread Spectrum Gains Wireless Applications," *Microwave & RF*, pp. 41. May 1992.

6. Qualcomm, "Proposed Wideband Spread-Spectrum Standard," Qualcomm, Mar. 1992.

7. Lam, A. W. and Tantarantana S., "Theory and Applications of Spread Spectrum Systems - A self-study course," IEEE Press, 1994.

8. Salmasi A. and Gilhousen K. S., "On the System Design Aspects of CDMA Applied to Digital Cellular and Personal Communications Networks," *41st. IEEE Vehicular Technologies Conference*, pp. 57-62, 1991.

INITIAL DISTRIBUTION LIST

No. Copies

1. Defense Technical Information Center 2
Cameron Station
Alexandria, Virginia 22304-6145

2. Library, Code 52 2
Naval Postgraduate School
Monterey, California 93943-5101

3. Chairman, Code EC 1
Department of Electrical and Computer Engineering
Naval Post Graduate School
Monterey, CA 93943-5121

4. Professor Alex W. Lam, Code EC/La 5
Department of Electrical and Computer Engineering
Naval Post Graduate School
Monterey, CA 93943-5121

5. Professor Donald v. Z. Wadsworth, EC/Wd 1
Department of Electrical and Computer Engineering
Naval Post Graduate School
Monterey, CA 93943-5121

6. Chief Defence Scientist 1
MINDEF Singapore
MINDEF Building, Gombak Drive, S2366
Republic of Singapore

7. Head, Air Logistics 1
HQ-RSAF, MINDEF
MINDEF Building, Gombak Drive, S2366
Republic of Singapore

8. Director 1
Defence Science Organisation
20 Science Park Drive, S0511
Republic of Singapore

9. Director 1
Defence Materials Organisation
LEO Building, Paya Lebar Airport, S1953
Republic of Singapore

10. MAJ Eugene Chang 2
HQ-RSAF, ALD
Paya Lebar Airport, S1953
Republic of Singapore

11. CAPT James R. Powell 1
J-33/STOD/C2W/EW
The Pentagon, 2C861
Washington, DC 20318-3000